BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Beberapa penelitian terdahulu yang pernah dilakukan untuk penilaian risiko IT menggunakan NIST SP 800-30 antara lain :

Dalam penelitian yang dilakukan oleh Aulia Febriyanti dan Bekti Cahyo Hidayanto (2012) yang membahas tentang pengelolaan data TI yang berbasis risiko pada PT. Petrokimia Gresik. Metode yang digunakan dalam mengelola risiko adalah NIST SP 800-30 yang dimulai dari mengidentifikasi risko, menilai risiko serta membentuk strategi untuk mengelolanya melalui sumber daya tersedia. Adapun beberapa permasalahan yang akan diangkat dalam penelitian ini yaitu bersifat korelasional dan deskriptif. Masalah dari penelitian yang dilakukan adalah risiko apa saja yang muncul selama proses pengelolaan data di bidang perkembangan TI di Tekinfo, dan dampak apa saja yang di timbulkan bagi risiko pada proses pengelolaan data yang sudah terintegrasi di bidang perkembangan TI di Tekinfo. Maka dapat disimpulakan bahwa pada proses pengelolahan data dihasilkan risiko-risiko yang sudah teridentifikasi dan risiko yang ada dalam proses pengelolaan keamanan sistem informasi seperti kebakaran, *virus, human error, hacking,* kehilangan data yang tidak berhasil di *backup* dan *restore, debugging* dan *revers engineering.* Sehingga diperoleh informasi berupa identifikasi ancaman yang berpotensial untuk menciptakan risiko bagi TI beserta dampak yang akan dihasilkan, dan mitigasi dengan menanggani risiko.

Dan penelitian selanjutnya dilakukan oleh Ovickma Yudianto, Fadjriah Julianti dan Tan Fredy (2010) yang melakukan pengukuran terhadap tingkat risiko teknologi informasi serta mengidentifikasi praktek-praktek keamanan yang cocok dalam penanggulangan risiko pada PT. Saga Machie dan diharapkan perusahaan dapat lebih wasapada terhadap dampak-dampak dari risiko teknologi informasi yang mungkin terjadi di dalam PT Saga Machie. Penelitian ini menggunakan metode NIST 800-30, metode ini digunakan dalam pengukuran risiko teknologi

informasi dengan beberapa langkah yang berperan penting dalam mencari hasil pengukuran secara efektif dan efesien. Hasil yang dicapai adalah memberikan keseluruhan hasil dari pengukuran risiko yang terjadi pada perusahaan baik kelebihannya maupun kekurangannya, serta memberikan rekomendasi-rekomendasi yang diharapkan dapat mengatasi dan memperbaiki kekurangan maupun permasalahan yang terjadi dalam PT Saga Machie.

2.2 Konsep Manajemen Risiko

2.2.1 Pengertian Risiko

Risiko merupakan kombinasi dari probabilitas suatu kejadian dan konsekuensi dari kejadian tesebut, dengan tidak menutup kemungkinan bahwa ada lebih dari satu konsekuensi untuk satu kejadian, dan konsekuensi bisa merupakan hal yang positif maupun negatif. (Shortreed, et al. 2003). namun risiko pada umumnya dipandang sebagai sesuatu yang negatif, seperti kehilangan, bahaya, dan konsekuensi lainnya. Kerugian tersebut sebenarnya merupakan bentuk ketidakpastian yang seharusnya dipahami dan dikelola secara efektif oleh organisasi sebagai bagian dari strategi sehingga dapat menjadi nilai tambah dan mendukung pencapaian tujuan organisasi.

2.2.2 Manajemen Risiko

Manajemen risiko didefinisikan sebagai proses, mengidentifikasi, mengukur dan memastikan risiko dan mengembangkan strategi untuk mengelola risiko tersebut. Dalam hal ini manajemen risiko akan melibatkan proses-proses, metode dan teknik yang membantu manajer proyek maksimumkan probabilitas dan konsekuensi event yang berlawanan.

Dalam manajemen proyek, yang dimaksud dengan manajemen risiko proyek adalah seni dan ilmu untuk mengidentifikasi, menganalisis, dan merespon risiko selama umur dan tetap menjamin tercapainya tujuan proyek.

2.2.3 Macam-macam Risiko

Menurut Gondodiyoto (2006,p302), ancaman terhadap keamanan dapat bersifat karena alam, manusia, yang berifat kelelalaian atau kesengajaan, antara lain :

a) Ancaman kebakaran

Beberapa pelaksanaan keamanan untuk ancaman kebakaran :

a. Memiliki alat pemadam kebakaran otomatis dan tabung pemadam kebakaran.
b. Memiliki pintu/tangga darurat
c. Melakukan pengecekan rutin dan pengujian terhadap sistem pelindungan kebakaran untuk dapat memastikan bahwa segala sesuatunya telah dirawat dengan baik.

b) Ancaman banjir

` Beberapa pelaksanaan pengamanan untuk ancaman banjir :

a. Usahkan bahan atap, dinding dan lantai yang tahan air
b. Semua material asset informasi di taruh di tempat yang tinggi
c. Perubahan tegangan sumber energi
d. Pelaksanaan pengaman untuk mengantisipasi perubahan tegangan sumber energi, misalnya : menggunakan *stabilizer atau power supplay (UPS).*

c) Kerusakan Strukural

Pelaksanaan pengaman untuk antisipasi kerusakan structural misalnya : memilih lokasi perusahaan yang jarang terjadi gempa, angin ribut, banjir.

d) Penyusup

Pelaksanaan pengamanan untuk mengantisipasi penyusup adalah penempatkan penjaga dan penggunaan alarm atau kamera pengawas.

e) Virus

Pelaksanaan pengamanan untuk mengantisipasi *virus* adalah :

a. *Preventif,* seperti memaang anti *virus* dan melakukan *update* secara rutin
b. *Detektif,* misalnya melakukan *scan file* sebelum digunakan.
c. *Korektif,* misalnya memastikan *backup* data bebas *virus*, pemakaian anti *virus* terhadap file yang terinfeksi.

f) *Hacking*

Beberapa pelaksanaan pengamanan untuk mengantisipasi hacking :

a. Penggunaan *control logical* seperti pengguanaan *password* yang sulit ditebak. Petugas keamanan secara teratur memonitori sistem yang digunakan.

g) Kegagalan jaringan, kegagalan sistem dan data

Beberapa pelaksanaan pengamanan untuk mengantisipasi risiko tersebut :

a. *Recovery Time Objectives* (RTO) adalah lama waktu yang dibutuhkan untuk pemulihan sistem dan data.Jika antar komponen layanan atau *service component* terjadi *dependency*, maka waktu recovery dihitung secara serial untuk komponen-komponen yang *interdepencency*.Jika antar komponen layanan tidak saling bergantung, *recovery time* dapat dihitung secara paralel antara komponen layanan.Maksimum RTO adalah 80% dari maksimum waktu layanan tidak befungsi yang ditoleransi atau MTDL.

b. *Recovery Point Objectives* (RPO) adalah ambang berapa banyak data yang boleh hilang sejak terakhir backup dilakukan. Jika *backup* dilakukan sekali sehari pada malam hari, sementara kerusakan sistem/*storage* dapat terjadi beberapa menit sebelum proses *backup* dijalankan, maka nilai RPO adalah 24 jam. Dengan kata lain RPO merupakan pernyataan berapa lama suatu informasi/data boleh hilang.

2.3 Manajemen Risiko Teknologi Informasi

Menurut Alberts dan Dorefee (2004), manajemen risiko adalah proses yang berkelanjutan dalam mengenal risiko dan mengimplementasikan rencana untuk menunjuk mereka.

Jadi, manajemen risiko adalah suatu proses identifikasi, mengukur risiko, serta membentuk strartegi untuk mengelolanya melalui sumber daya yang tersedia. Strategi yang dapat digunakan antara lain mentransfer risiko pada pihak

lain, menghindari risiko, mengurangi efek buruk dari risiko, dan menerima sebagian maupun seluruh konsekuensi dari risiko tertentu.

2.3.1 Kategori Risiko Teknologi Informasi

Menurut Hughes (2006: 36) di dalam Gui, Anderes et al (2008), kategori risiko TI antara kehilangan informasi potensial dan pemulihannya adalah sebagai berikut.

a) Pertama adalah keamanan. Risiko yang informasinya diubah atau digunakan oleh orang yang tidak berotoritas. Ini termasuk kejahatan komputer, kebocoran internal, dan terorisme *cyber*.
b) Kedua adalah ketersediaan. Risiko yang datanya tidak dapat diakses seperti setelah kegagalan sistem, karena kesalahan manusia, perubahan konfigurasi, kurangnya pengurangan arsitektur atau akibat lainnya.
c) Ketiga adalah daya pulih. Risiko di mana informasi yang diperlukan tidak dapat dipulihkan dalam waktu yang cukup, setelah sebuah kejadian keamanan atau ketersediaan seperti kegagalan perangkat lunak atau keras, ancaman eksternal, atau bencana alam.
d) Keempat adalah *performa*. Risiko di mana informasi tidak tersedia saat diperlukan, yang diakibatkan oleh arsitektur terdistribusi, permintaan yang tinggi, dan topografi informasi teknologi yang beragam.
e) Kelima adalah daya skala. Risiko yang perkembangan bisnis, pengaturan *bottleneck*, dan bentuk arsitekturnya membuatnya tidak mungkin menangani banyak aplikasi baru dan biaya bisnis secara efektif.
f) Keenam adalah ketaatan. Risiko yang manajemen atau penggunaan informasinya melanggar keperluan *regulator*. Yang dipersalahkan dalam hal ini mencakup regulasi pemerintah, panduan pengaturan korporat, dan kebijakan internal.

2.4 Pengertian Kemanan Informasi

Berdasarkan buku Riyananto Sarno dan Irsyaf Iffano (2009) informasi merupakan aset seharusnya dilindungi agar aman. Keamanan secara umum

diartikan sebagai kondisi yang terbebas dari ancaman atau bahaya. Secara logika untuk menjadi aman adalah dengan cara dilindungi dari ancaman dan bahaya.

Sedangkan keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimalkan risiko bisnis dan memaksimalkan atau mempercepat pengambilan investasi dan peluang bisnis (ISO/IEC 27001,2005).

Kemanan bisa dicapai dengan beberapa cara atau strategi yang bisa dilakukan secara simultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi-strategi dari keamanan informasi masing-masing memiliki fokus dan bangun tujuan tertentu sesuai kebutuhan.

2.4.1 Aspek Kemanan Informasi

Kemanan informasi terkait erat dengan fasilitas pemprosesan infomasi yang meliputi dokumen, perangkat keras, perangkat lunak, infrastruktur dan bangunan yang melindunginya. Hal tersebut seharusnya direncanakan dan dikoodinasikan dengan baik agar dapat melindungi sumber daya dan investasi lainnya. Pelindungan pada informasi tersebut dilakukan untuk memenuhi aspek keamanan informasi. Untuk aspek kemanan informasi meliputi tiga yaitu :

a) *Confidentiality* : keamanan informasi seharusnya bisa menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tertentu.
b) *Integrity* : keamanan informasi seharusnya menjamin kelengkapan informasi dan menjaga dari korupsi, kerusakan, atau ancaman lain yang menyebabkannya berubah informasi dari aslinya.
c) *Availability* : keamanan informasi seharusnya menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tak bisa digunakan. Pengguna, dalam hal ini bisa jadi manusia, atau komputer yang tentunya dalam hal ini memiliki otoritasi untuk mengakses.

2.4.2 Keamanan Sistem dan Teknologi

Berdasarkan buku Janner Simarmata (2006) keamanan sistem mengacu pada perlindungan terhadap semua sumber daya informasi perusahaan dari

ancaman pihak-pihak yang tidak berhak.

Keamanan berhubungan dengan orang-orang yang mencoba mengakses *remote* secara ilegal. Sebagian besar masalah keamanan terutama disebabkan oleh orang jahat yang mencoba mengambil keuntungan atau mengganggu seseorang.

Informasi yang digunakan oleh bisnis dapat berupa *record* komputer, kertas, model skala, *prototipe* dan lain

2.4.3 Tujuan Utama Menyediakan Keamanan

a) Kerahasiaan (*confidentiality*) adalah keterjaminan bahwa informasi pada sistem komputer hanya dapat diakses oleh pihak-pihak otoritas dan modifikasi dilakukan dengan tetap menjaga keutuhan dan konsistensi data sistem tersebut.
b) Integritas (*integrity*) adalah keterjaminan bahwa sumber sistem hanya dapat di modifikasi oleh pihak-pihak yang otoritas.
c) Ketersediaan (*availability*) adalah keterjaminan bahwa sumber daya sistem komputer telah tersedia bagi pihak-pihak yang diotoritasi saat diperlukan.

2.5 Pengertian Ancaman, Kemungkinan dan Dampak

2.5.1 Ancaman

Menurut NIST SP 800-30 (2012). Ancaman adalah setiap keadaan atau peristiwa yang berpotensi menimbulkan dampak merugikan terhadap operasi aset, individu dan organisasi lain melalui akses yang tidak sah, perusakan, pengungkapan atau modifikasi informasi. Peristiwa ancaman yang disesbabkan oleh sumber-sumber ancaman.

2.5.2 Kemungkinan

Menurut NIST SP 800-30 (2012). Kemungkinan kejadian adalah faktor risiko bertimbang berdasarkan analisis probabilitas bahwa ancaman yang diberikan mampu memanfaatkan kerentanan yang diberikan (atau serangakaian kerentanan). Faktor risiko kemungkinan menggabungkan perkiraan kemungkinan bahwa peristiwa ancaman akan mulai dengan perkiraan kemungkinan dampak yaitu : kemungkinan bahwa hasil kejadian ancaman dampak yang meruginkan.

2.5.3 Dampak

Dampak menurut KBBI adalah benturan, pengaruh yang mendatangkan akibat baik positf maupun negatif.

Pengaruh adalah daya yang ada dan timbul dari sesuatu (orang benda) yang ikut membentuk watak, kepercayaan atau perbuatan seseorang pengaruh adalah suatu keadaan dimana ada hubungan timbal balik atau hubungan sebab akibat antara apa yang mempengaruhi dengan apa yang dipengaruhi. (KBBI Online, 2010)

2.6 Penanganan Risiko

Penanganan risiko adalah proses yang dilakukan untuk meminimalisasi tingkat risiko yang dihadapi sampai pada batas yang dapat diterima. Secara kuantitatif upaya untuk meminimalisasi risiko ini dilakukan dengan menerapkan langkah-langkah yang diarahkan pada turunnya (angka) hasil ukur yang diperoleh dari proses analisa risiko. Pemilihan penanganan risiko yang terbaik akan diperlukan.

2.6.1 Teknik Menangani Risiko

a. Menghindari Risiko

   Cara ini dilakukan dengan tidak melakukan aktifitas yang mendatangkan risiko. Dalam hal pengerjaan proyek bisa dilakukan dengan cara merubah rencana proyek untuk menghilangkan risiko. Meskipun tidak semua risiko bisa dihindari, beberapa risiko masih mungkin menghindar. Beberapa risiko yang mungkin terjadi di tahap awal proyek bisa dihindari dengan mengklarifikasi keburuhan proyek, mengumpulkan informasi, memperbaiki komunikasi atau memperbaiki kemampuan.

b. Reduksi Risiko

   Meliputi langkah-langkah untuk mengurangi peluang terjadinya risiko. Melakukan tindakan awal untuk mengurangi peluang terjandinya risiko pada proyek akan lebih efektif daripada memperbaiki setelah suatu kejadian berisiko terjadi.

c. Menerima Risiko

Menerima kerugian jika kejadian yang berisiko terjadi. Ini bisa dilakukan jika risiko yang ditimbulkan kecil. Atau tidak ada cara lain lagi untuk menangani. Penerimaan risiko secara aktif bisa diwujudkan dengan menyiapkan rencana *contingency* atau cadangan jika risiko yang diperkirakan terjadi.

d. *Transfer* Risiko

Mengalihkan risiko ke pihak lain. Cara yang umum dalam bisnis adalah membeli asurasi. Dengan asuransi, kita berusaha mengalihkan risiko ke pihak lain. Bisa saja penganganan suatu risiko jatuh ke beberapa kategori. Misalnya mengurangi risiko sekaligus mengalihkan risiko.

2.6.2 Penilaian Risiko

Menurut Soehatman Ramli (2010) di dalam bukunya menyatakan hasil identifikasi bahaya selanjutnya dianalisa dan dievaluasi untuk menentukan besarnya risiko serta tingkat risiko dan menentukan apakah risiko tersebut dapat diterima atau tidak.

2.7 Metode Pengukuran Risiko Teknologi Informasi

Dalam melakukan proses pengukuran risiko teknologi informasi penulis membutuhkan metode yang dapat dijadikan pedoman. Berikut adalah beberapa metode yang tersedia dalam melakukan pengukuran risiko keamanan teknologi informasi. Diantaranya metode NIST SP 800-30, OCTAVE- S, dan COBIT untuk perbandingan.

2.7.1 Pengukuran Risiko Teknologi Berdasarkan NIST (*National Institute of Standard and Technology*) Special Publication 800-30

NIST (*National Institute of Standard and Technology*) mengeluarkan rekomendasi melalui publikasi khusus 800 – 30, panduan manajemen risiko untuk sistem teknologi informasi yang merupakan standar pemerintah federal US. Metodologi ini terutama dirancang untuk menjadi suatu perhituangan kualitatif. Proses ini sangat komprehensif, meliputi segala sesuatu dari sumber ancaman identifikasi untuk evaluasi berkelanjutan dan penilaian. Metodologi NIST proses

penilaian risiko terdiri dari 9 langkah sebagai berikut :

HIPAA (2012) menjelaskan mengenai panduan dalam menggunakan metode NIST (*National Institute of Standard and Technology*) Special Publication (SP) 800-30. Berikut adalah penjelasan lebih rinci mengenai sembilan langkah pada metode NIST.

1. Karakterisasi sistem

   Langkah pertama dalam menilai risiko adalah untuk menentukan ruang lingkup usaha. Untuk melakukan hal ini, mengidentifikasi di mana dibuat, diterima, dipelihara, diproses, atau ditransmisikan. Menggunakan teknik pengumpulan informasi, batasan sistem TI diidentifikasi, serta sumber daya dan informasi yang merupakan bagian dari sistem. Mempertimbangkan kebijakan , hukum, tenaga kerja dan telecommuters, dan media *removable* dan perangkat komputasi portabel (misalnya, laptop, *media removable*, dan media *backup*). *Output* - Karakterisasi dari sistem TI dinilai, gambar yang bagus dari lingkungan sistem IT, dan batas sistem

2. Identifikasi ancaman

   Untuk langkah ini, potensi ancaman (potensi sumber ancaman untuk berhasil melaksanakan kerentanan tertentu) diidentifikasi dan didokumentasikan. Sumber ancaman adalah setiap keadaan atau peristiwa dengan potensi untuk menyebabkan kerusakan pada sistem IT (disengaja atau tidak disengaja). Sumber ancaman secara umum dapat dari alam, manusia, atau pertimbangan lingkungan. semua potensi ancaman - sumber, melihat kembali kejadian sebelumnya dan data dari badan-badan intelijen, pemerintah, dll, membantu menghasilkan *item* untuk dimasukkan pada daftar. Daftar berdasar pada organisasi secara individu dan pengolahan lingkungan. *Output* - Sebuah pernyataan ancaman yang berisi daftar ancaman - sumber yang dapat mengeksploitasi sistem kerentanan.

3. Identifikasi kerentanan

   Tujuan dari langkah ini adalah untuk mengembangkan daftar kerentanan sistem teknis dan non-teknis (kekurangan atau kelemahan) yang dapat

dimanfaatkan atau dipicu oleh sumber-sumber ancaman - potensial. Kerentanan dapat berkisar dari kebijakan yang tidak lengkap atau bertentangan yang mengatur penggunaan komputer organisasi untuk perlindungan memadai untuk melindungi fasilitas peralatan komputer ke sejumlah perangkat lunak, perangkat keras, atau kekurangan lain yang terdiri dari jaringan komputer organisasi. *Output* - Sebuah daftar kerentanan sistem (pengamatan) yang dapat dieksekusi oleh sumber ancaman-potensial.

4. Analisis pengendalian

   Tujuan dari langkah ini adalah untuk mendokumentasikan dan menilai efektivitas pengendalian teknis dan non-teknis yang telah atau akan dilaksanakan oleh organisasi untuk meminimalkan atau menghilangkan kemungkinan (probabilitas atau) dari sumber ancaman - mengeksploitasi kerentanan sistem. *Output* - Daftar kontrol saat ini atau yang direncanakan (kebijakan, prosedur, pelatihan, mekanisme teknis, asuransi, dll) yang digunakan untuk sistem TI untuk mengurangi kemungkinan kerentanan yang dilakukan dan mengurangi dampak seperti sebuah peristiwa yang merugikan.

5. Penentuan kemungkinan

   Tujuan dari langkah ini adalah untuk menentukan nilai keseluruhan kemungkinan yang menunjukkan kemungkinan bahwa kerentanan dapat dimanfaatkan oleh sumber ancaman yang diberikan kontrol keamanan yang ada atau yang direncanakan. Output - Kemungkinan rating rendah (1-3), menengah (4-8), atau tinggi (9-14). Rujuk ke NIST SP 800-30 definisi rendah, menengah, dan tinggi.

   Berikut ini faktor-faktor yang harus dipertimbangkan :

   a) Motivasi dan sumber ancaman
   b) Sifat dari kerentanan
   c) Keberadaan dan efektifitas pengendalian saat ini

Tabel 2.1 : Definisi kemungkinan/ kecendrungan

Level Kemungkinan	Definisi kemungkinan/kecenderungan
Tinggi	Sumber ancaman yang memiliki motivasi tinggi, memiliki kemampuan yang cukup, dan pengendalian untuk mencegah kerentanan yang mungkin terjadi tidak efektif.
Sedang	Sumber ancaman termotivasi dan mampu, tetapi pengendalian yang ada, dapat menghambat kerentanan dengan sukses.
Rendah	Sumber ancaman kurang termotivasi dan mampu, atau pengendalian yang ada untuk mencengah atau setidaknya secara signifikan menghambat kerentanan yang mungkin terjadi

6. Analisis Dampak

Tujuan dari langkah ini adalah untuk menentukan tingkat dampak negatif yang akan dihasilkan dari ancaman berhasil mengeksploitasi kerentanan. Faktor data dan sistem untuk mempertimbangkan harus mencakup pentingnya misi organisasi, kepekaan dan kekritisan (nilai atau kepentingan), biaya yang terkait, hilangnya kerahasiaan, integritas, dan ketersediaan sistem dan data. *Output* - Besaran Peringkat dampak rendah (1), sedang (2-3), atau tinggi (4-5). Rujuk ke SP NIST 800-30 definisi rendah, sedang, dan tinggi.

Tabel 2.2 : Definisi Besarnya Dampak

Besarnya Dampak	Definisi dampak
Tinggi	Penerapan kerentanan: (1) dapat menghasilkan kehilangan biaya yang sangat tinggi dari aset nyata

	utama atau sumber daya, (2) dapat menyebabkan pelanggaran, kerugian atau rintangan dalam misi organisasi, reputasi atau pendapatan yang signifikan, (3) dapat menyebabkan kematian atau cedera serius.
Sedang	Penerapan kerentanan: (1) dapat menghasilkan kehilangan biaya yang tinggi dari aset nyata utama atau sumber daya, (2) dapat menyebabkan pelanggaran, kerugian atau rintangan dalam misi organisasi, reputasi atau pendapatan, (3) dapat menyebabkan cedera serius.
Rendah	Penerapan kerentanan: (1) dapat menghasilkan kehilangan sebagian aset nyata atau sumberdaya, (2) dapat mempengaruhi misi, reputasi dan pendapatan organisasi.

7. Penentuan risiko

   Dengan mengalikan peringkat dari penentuan kemungkinan dan analisis dampak, tingkat risiko ditentukan. Ini merupakan derajat atau tingkat risiko yang bersistem TI, fasilitas, atau prosedur mungkin terkena jika kerentanan yang diberikan telah dieksekusi. Peringkat risiko juga menyajikan tindakan manajemen senior (pemilik misi) yang harus diambil untuk setiap tingkat risiko. *Output* - Risiko tingkat rendah (1-3), sedang (4-6) atau tinggi (7-9). Rujuk ke SP NIST 800-30 definisi rendah, sedang, dan tinggi.

   Rumus : Penilaian Risko = Dampak x Peluang

Tabel 2.3 : Tingkat Risiko

Skor	Tingkat Risiko	Deskripsi Risiko dan Tindakan Diperlukan
7-9	Tinggi	Jika observasi atau temuan dievaluasi sebagai risiko tinggi, ada kebutuhan yang kuat untuk langkah-langkah perbaikan. Sistem yang ada dapat terus beroperasi, tetapi rencana tindakan korektif harus diletakkan di tempat secepat mungkin.
4-6	Sedang	Jika pengamatan dinilai sebagai Risiko sedang, harus mendapat perlakuan untuk perbaikan, mencegah dan menguranginya. Dan dapat diberikan kontrol yang sesuai dalam jangka waktu yang wajar.
1-3	Rendah	Jika pengamatan di nilai risiko rendah, maka Risiko dapat diterima dan untuk kedepanya akan dilakukan eskalasi lebih lanjut terhadap kontrol.

8. Rekomendasi kontrol

   Tujuan dari langkah ini adalah untuk mengidentifikasi kontrol yang dapat mengurangi atau menghilangkan risiko yang teridentifikasi, sesuai dengan operasi organisasi. Tujuan dari kontrol ini adalah untuk mengurangi tingkat risiko terhadap sistem dan data ke tingkat yang dapat diterima. Faktor-faktor yang perlu dipertimbangkan ketika mengembangkan kontrol mungkin termasuk efektivitas atas pilihan yang direkomendasikan (yaitu, kompatibilitas sistem), undang-undang dan peraturan, kebijakan organisasi, dampak operasional, dan keselamatan dan keandalan. Rekomendasi kontrol memberikan masukan untuk proses mitigasi risiko, di mana kontrol direkomendasikan keamanan prosedural dan teknis dievaluasi, diprioritaskan, dan diimplementasikan. *Output* - Rekomendasi

kontrol(*s*) dan solusi alternatif untuk mengurangi risiko.

9. Dokumentasi hasil

   Hasil dari penilaian risiko yang didokumentasikan dalam laporan resmi atau *briefing* dan diberikan kepada manajemen senior (pemilik misi) untuk membuat keputusan tentang kebijakan, prosedur, anggaran, dan sistem perubahan operasional dan manajemen. *Output* - Sebuah laporan penilaian risiko yang menggambarkan ancaman dan kerentanan, mengukur risiko, dan memberikan rekomendasi untuk pelaksanaan kontrol. Setelah menyelesaikan proses sembilan langkah penilaian risiko, langkah berikutnya adalah mitigasi risiko. *Mitigasi* risiko melibatkan memprioritaskan, mengevaluasi, dan menerapkan sesuai mengurangi risiko kontrol direkomendasikan dari proses penilaian risiko.

2.8 Profil Perusahaan PT. Perkebunan Nusantara V

Nama	:	PT. Perkebunan Nusantara V (Persero)
Bidang Usaha	:	Agrobisnis dan agro industri kelapa sawit dan karet.
Kepemilikan	:	Pemerintahan Republik Indonesia 100%
Tanggal Pendiri	:	11 Maret 1996
Dasar Hukum Pendirian	:	Peraturan Pemerintahan Republik Indonesia No. 10 Tahun 1996
Modal Dasar	:	Rp. 5.200.000.000 (lima triliun dua ratus milliar rupiah) terbagi atas 5.200.00 (lima juta dua ratus ribu) lembar saham, masing-masing saham dengan nilai nominal sebesar Rp 1.000.000 (satu juta rupiah).
Modal Ditempatkan Dan Disetor Penuh	:	1.313.322 (satu juta tiga ratus tiga belas ribu tiga ratus dua puluh dua saham) lembar saham atau seluruhnya sebesar Rp 1.313.322.000.000 ((satu juta tiga ratus tiga belas ribu tiga ratus dua puluh dua).

Kantor pusat	:	Jl. Rambutan No. 43 Pekanbaru-Riau 28294 Tlp.(62-761), Fax (62-761) 66558 Email : ptpn5@ptpn5.co.id Website : www.ptpn5.com
Kantor perwakilan	:	Jl. Cempaka Putih Tengah XXX No. 73 Jakarta Pusat-10510 Tlp. (62-21) 4244291, Fax (62-21) 4245034

2.8.1 Sejarah Berdirinya Perusahaan

PT Perkebunan Nusantara V (Persero) "perusahaan" merupakan BUMN Perkebunan yang didirikan tanggal 11 Maret 1996 sebagai hasil konsilidasi kebun pengembangan PTP II, PTP IV ,dan PTP V di Provinsi Riau. Secara efektif Perusahaan mulai beroperasi sejak tanggal 9 April 1996 dengan kantor pusat di Pekanbaru. Landasan hukum perusahaan ditetapka berdasarkan peraturan Pemerintah Republik Indonesia No. 10 Tahun 1996 tentang Penyetoran Modal Negara Republik Indonesia untuk Pendirian Perusahaan Perseroan (Persero) PTPN V.

Anggaran Dasar Perusahaan dibuat di depan Notaris Harun Kamil melalui Akte No. 38 tanggal 11 Maret 1996 dan disahkan melalui Keputusan Menteri Kehakiman RI No. C2-8333H.T.01 Tahun 1996, serta telah diumumkan dalam Berita Negara Republik Indonesia (RI) Nomor 8565/1996. Anggaran Dasar Perseroan telah beberapa kali mengalami perubahan, terakhir dengan akta Notaris Budi Suyono, SH No.70 tanggal 15 Oktober 2012. Perubahan anggaran Dasar tersebut untuk mengakomodasi perubahan Modal Dasar dan perubahan Modal Ditempatkan dan Disetor penuh Perseroan. Perusahaan ini telah mendapatkan persetuan Menteri Hukum dan HAM Republik Indonesia melalui Surat Keputusan No. AHU-04539.AH.01.02 Tahun 2013 tentang Persetujuan Perubahan Anggaran Dasar.

Saat ini Kantor Pusat Perseroan berkedudukan di Jl. Rambutan No.43 Pekanbaru, dengan unit-unit usaha yang tersebar di berbagai Kabupaten di Provinsi Riau. Hingga tahun 2012, Perseroan mengelola 47 unit kerja yang terdiri dari 1 unit Kantor Pusat, 4 *Strategic Business* Unit (SBU), 20 unit Kebun Inti, 3 manajemen kebun plasma, 12 Pabrik kelapa sawit (PKS) 1 unit pabrik PKO, 3

fasilitas Pengelolahan Karet, dan 3 Rumah Sakit. Areal yang dikelola oleh Perseroan seluas 161.541 Ha, yang terdiri dari 87.015 Ha lahan sendiri/inti dan 74.526 Ha lahan plasma.

PT Perkebunan Nusantara V (Persero) “perusahaan” merupakan BUMN Perkebunan yang didirikan tanggal 11 Maret 1996 sebagai hasil konsilidasi kebun pengembangan PTP II, PTP IV ,dan PTP V di Provinsi Riau. Secara efektif Perusahaan mulai beroperasi sejak tanggal 9 April 1996 dengan kantor pusat di Pekanbaru. Landasan hukum perusahaan ditetapka berdasarkan peraturan Pemerintah Republik Indonesia No. 10 Tahun 1996 tentang Penyetoran Modal Negara Republik Indonesia untuk Pendirian Perusahaan Perseroan (Persero) PTPN V.

Anggaran Dasar Perusahaan dibuat di depan Notaris Harun Kamil melalui Akte No. 38 tanggal 11 Maret 1996 dan disahkan melalui Keputusan Menteri Kehakiman RI No. C2-8333H.T.01 Tahun 1996, serta telah diumumkan dalam Berita Negara Republik Indonesia (RI) Nomor 8565/1996. Anggaran Dasar Perseroan telah beberapa kali mengalami perubahan, terakhir dengan akta Notaris Budi Suyono, SH No.70 tanggal 15 Oktober 2012. Perubahan anggaran Dasar tersebut untuk mengakomodasi perubahan Modal Dasar dan perubahan Modal Ditempatkan dan Disetor penuh Perseroan. Perusahaan ini telah mendapatkan persetuan Menteri Hukum dan HAM Republik Indonesia melalui Surat Keputusan No. AHU-04539.AH.01.02 Tahun 2013 tentang Persetujuan Perubahan Anggaran Dasar.

Saat ini Kantor Pusat Perseroan berkedudukan di Jl. Rambutan No.43 Pekanbaru, dengan unit-unit usaha yang tersebar di berbagai Kabupaten di Provinsi Riau.

Hingga tahun 2012, Perseroan mengelola 47 unit kerja yang terdiri dari 1 unit Kantor Pusat, 4 Strategic Business Unit (SBU), 20 unit Kebun Inti, 3 manajemen kebun plasma, 12 Pabrik kelapa sawit (PKS) 1 unit pabrik PKO, 3 fasilitas Pengelolahan Karet, dan 3 Rumah Sakit. Areal yang dikelola oleh Perseroan seluas 161.541 Ha, yang terdiri dari 87.015 Ha lahan sendiri/inti dan 74.526 Ha lahan plasma.

2.8.2 Visi dan Misi

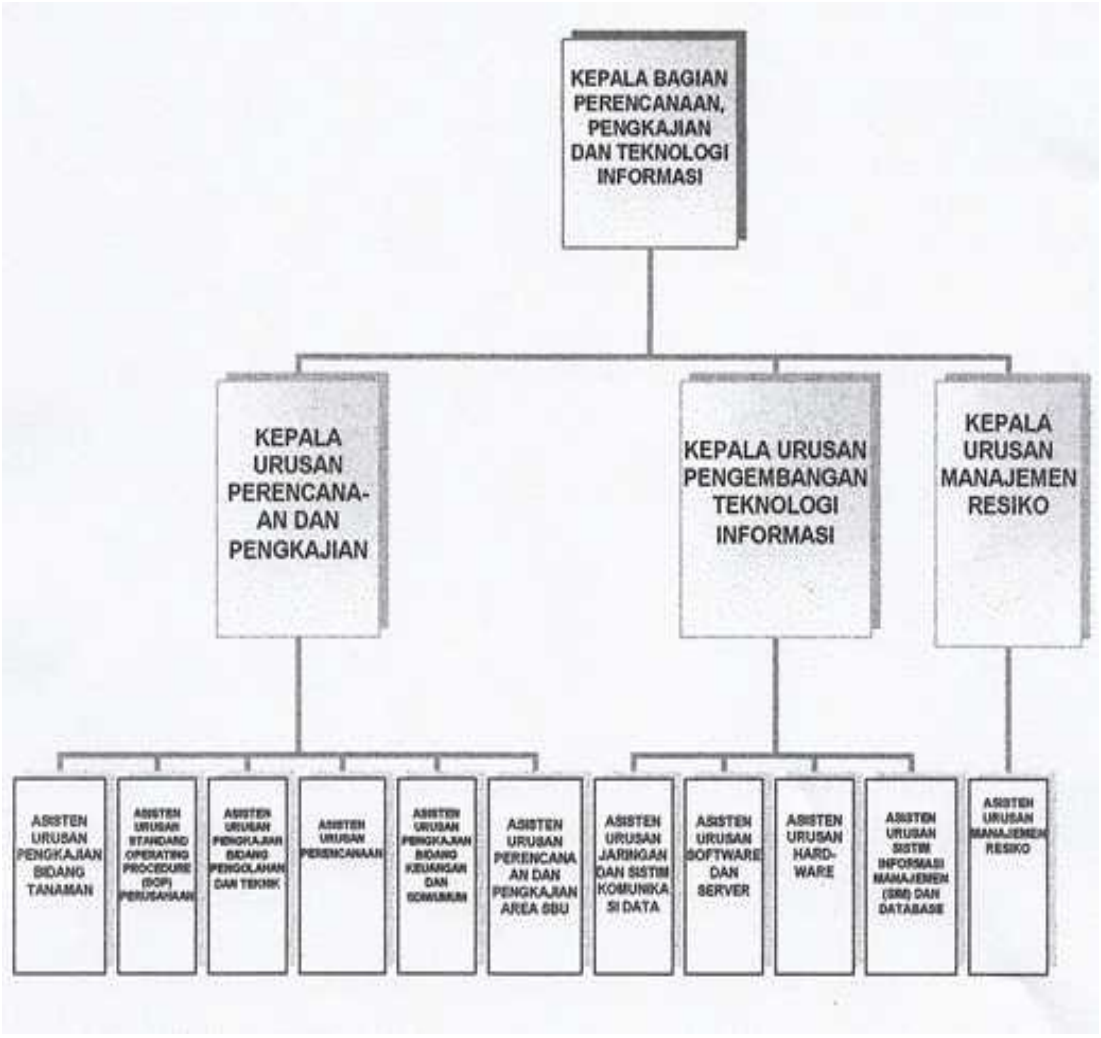
a. Visi

Menjadi perusahaan perkebunan yang tangguh, mampu tumbuh dan berkembang dalam persaingan global.

b. Misi

Mengelola agroindustri kelapa sawit dan karet secara efisien bersama mitra, untuk kepentingan *stakeholder*, berwawasan lingkungan, berdasarkan prinsip-prinsip *Good Corporate* dan *Governance* dan menciptakan nilai tambah perusahaan secara berkelanjutan.

2.8.3 Struktur Organisasi Bagian Perencanaan dan Pengembangan Teknologi Informasi



Gambar 2.2 Struktur Organisasi Bagian P2TI

2.8.4 Deskripsi Pekerjaan

a. Jabatan Kepala Bagian Perencanaan, Pengkajian dan Teknologi Informasi

Tugas Pokok :

1. Menyusun pedoman RKAP yang terkait dengan perencanaan, pengkajian dan teknologi informasi.
2. Menyusun *program* kegiatan dan anggaran Bagian Perencanaan, Pengkajian dan Teknologi Informasi.
3. Mengkoordinir penyusunan Rencana Jangka Panjang Perusahaan (RJPP) dan mengadakan revisi RJP secara berkala sesuai kebutuhan.
4. Melaksanakan pengkajian aspek teknis, sistem dan prosedur di bidang tanaman, pengolahan/teknik, keuangan, SDM/Umum, dan kajian pengembangan teknologi informasi sesuai dengan rencana kerja yang sudah dibuat.
5. Melaksanakan pengkajian terhadap rencana penerapan sistem dan teknologi baru atau pengembangan sistem dan teknologi baru di bidang tanaman, pengolahan/teknik, keuangan, dan SDM/Umum.
6. Melaksanakan pengkajian atas permintaan Bagian/Unit apabila Bagian/Unit tersebut menghadapi masalah yang memerlukan pengkajian lebih lanjut.
7. Menyusun laporan setiap pelaksanaan kegiatan pengkajian yang dilakukan.
8. Melakukan *monitoring* dan evaluasi terhadap hasil kajian yang diimplementasikan oleh Bagian/Unit.
9. Melakukan evaluasi dan uji kelayakan terhadap teknologi informasi yang akan diterapkan di perusahaan.
10. Mengelola pengembangan sistem dan pemeliharaan seluruh perangkat keras (*hardware*), perangkat lunak *(sofware*) serta *peripheral equipment* di perusahaan.
11. Mengelola informasi dalam *situs website* internet dan *intranet*, portal BUMN *online* dan *web* LPP baik informasi yang bersifat umum maupun informasi teknis yang berkaitan dengan kegiatan perusahaan.
12. Mengelola pengembangan *program-program aplikasi* untuk menunjang efektivitas proses bisnis di perusahaan.

13. Memeriksa/mengevaluasi permintaan *hardware* dan *sofware* dari Bagian, SBU/Unit.
14. Menilai prestasi kerja Kepala Urusan dan mengevaluasi hasil penilaian prestasi kerja Asisten Urusan yang dinilai oleh Kepala Urusan serta penilaian prestasi kerja seluruh karyawan pelaksana yang dinilai oleh Asisten Urusan.
15. Membuat laporan berkala kegiatan Bagian.

b. Kepala Urusan Pengembangan Teknologi Informasi

Tugas pokok :

1. Menyusun pedoman RKAP Bidang Teknologi Informasi.
2. Menyusun program kegiatan dan anggaran Urusan Pengembangan Teknologi Informasi.
3. Melakukan pengkajian dalam pengembangan dan *aplikasi* teknologi informasi di perusahaan.
4. Membuat kajian untuk perencanaan dan disain jaringan komunikasi yang digunakan dalam *implementasi* sistem informasi manajemen berbasis komputer dan jaringan komunikasi *(net working)*.
5. Melakukan kajian untuk perancangan dan pengembangan basis data *(data base)* dan aliran data *(data flow)* yang digunakan dalam implementasi SIM berbasis komputer dan jaringan komunikasi.
6. Melakukan evaluasi dan uji kelayakan terhadap teknologi informasi yang akan diterapkan di perusahaan.
7. Menyusun sistem dan melaksanakan pemeliharaan seluruh perangkat keras *(hardware)* dan perangkat lunak *(sofware)* serta *peripheral equipment* jaringan komunikasi data yang ada di perusahaan.
8. Mengelola informasi dalam situs *website* internet dan intranet baik informasi yang bersifat umum maupun informasi teknis yang berkaitan dengan kegiatan perusahaan.
9. *Meng-update* materi (*conten)* informasi di portal BUMN *online* dan *web* LPP.
10. Menyusun dan mengembangkan program-program aplikasi untuk menunjang efektivitas proses bisnis di perusahaan.
11. Memeriksa/mengevaluasi permintaan *hardware* dan *sofware* dari Bagian, SBU/Unit.

12. Melakukan sosialisasi dan bimbingan teknis dalam implementasi aplikasi teknologi informasi dan program-program aplikasi.
13. Menilai prestasi kerja Asisten Urusan serta mengevaluasi penilaian prestasi kerja seluruh karyawan pelaksana yang dinilai oleh Asisten Urusan.
14. Membuat laporan pelaksanaan program dan kegiatan Urusan Pengembangan Teknologi Informasi.

c. Jabatan Asisten Urusan Jaringan Dan Sistem Komunikasi Data

Tugas Pokok :

1. Menyiapkan *draf program* kegiatan dan anggaran teknologi informasi.
2. Membuat kajian tentang perencanaan atas kebutuhan dan spesifikasi jaringan lokal area *network (LAN), Wide Area Network (WAN)* dan komunikasi data yang akan diterapkan perusahaan.
3. Membuat SOP tentang pemanfaatan infrastruktur *LAN , WAN* dan jaringan komunikasi data di perusahaan.
4. Membuat kajian perencanaan dan disain/arsitektur jaringan komunikasi data yang digunakan dalam sistem informasi manajemen berbasis komputer dan jaringan komunikasi *(net working)*.
5. Memelihara/menjamin koneksitas komunikasi data di lingkungan perusahaan.
6. Mengatur akses , mengelola bandwith dan koneksi internet perusahaan.
7. Mengoperasikan dan memelihara perangkat pendukung *LAN , WAN* dan komunikasi data.
8. Menjamin keamanan jaringan dan lalu lintas data pada sistem *LAN*, *WAN* dan sistem komunikasi data
9. Mengadakan evaluasi dan uji kelayakan terhadap perangkat keras *(hardware)* yang berkaitan dengan jaringan komunikasi data yang akan digunakan di perusahaan.
10. Membuat evaluasi dan uji kelayakan terhadap perangkat lunak (*sofware*) untuk pengoperasian jaringan *(networking operation system)* yang akan digunakan di perusahaan.
11. Menilai prestasi kerja seluruh karyawan pelaksana yang menjadi tanggung jawabnya.
12. Menyiapkan *draft* laporan pelaksanaan program dan kegiatan Urusan.

d. Jabatan Asisten *Software* Dan *Server*

Tugas Pokok :

1. Menyiapkan *draf program* kegiatan dan anggaran teknologi informasi.
2. Menyusun dan mengembangkan program-program *aplikasi (software)* untuk menunjang efektivitas proses bisnis di perusahaan.
3. Melakukan analisis dan evaluasi atas kelayakan program *aplikasi (software)* yang akan dipakai di perusahaan.
4. Merancang dan mengembangkan basis data *(data base)*, aliran data *(data flow)* dan program aplikasi yang digunakan dalam implementasi SIM berbasis komputer dan jaringan komunikasi.
5. Membuat dokumentasi dan SOP program aplikasi *(software)* yang telah selesai dikerjakan.
6. Memelihara, merawat dan mem-*backup program aplikasi* dan *server data base*.
7. Melakukan sosialisasi dan bimbingan teknis dalam implementasi aplikasi teknologi informasi dan program-program aplikasi *(software)*.
8. Mengelola sistem email *server* perusahaan.
9. Menilai prestasi kerja seluruh karyawan pelaksana yang menjadi tanggung jawabnya.
10. Menyiapkan *draft* laporan pelaksanaan program dan kegiatan Urusan.

e. Asisten Urusan *Hardware*

Tugas Pokok :

1. Menyiapkan *draf program* kegiatan dan anggaran teknologi informasi.
2. Membuat kajian tentang perencanaan atas kebutuhan dan spesifikasi perangkat keras komputer *(hardware)* dan *peripheral* untuk mendukung implementasi SIM berbasis komputer dan jaringan komunikasi.
3. Melakukan evaluasi atas kelayakan terhadap perangkat keras (komputer dan *peripheralnya*) yang akan digunakan di perusahaan.
4. Melaksanakan pememeliharaan seluruh perangkat komputer dan *peripheralnya*, baik yang bersifat *stand alone* maupun yang digunakan dalam jaringan komunikasi data di perusahaan.
5. Menyusun pedoman teknis penggunaan *hardware* di perusahaan.

6. Mengevaluasi kinerja perangkat keras komputer *(hardware)* yang digunakan perusahaan.
7. Memeriksa/mengevaluasi permintaan *hardware* dan *peripheralnya* dari Bagian, SBU/Unit.
8. Melakukan sosialisasi dan bimbingan teknis dalam hal perawatan perangkat keras komputer *(hardware).*
9. Menilai prestasi kerja seluruh karyawan pelaksana yang menjadi tanggung jawabnya.
10. Menyiapkan *draft* laporan pelaksanaan program dan kegiatan Urusan.

f. Asisten Urusan Sistem Informasi Manajemen dan *Databases*

Tugas Pokok :

1. Menyiapkan *draf program* kegiatan dan anggaran teknologi informasi.
2. Membuat kajian tentang perencanaan atas kebutuhan dan spesifikasi pengembangan SIM berbasis komputer dan *software DBMS* (*Database Management System*) yang akan diterapkan perusahaan.
3. Membuat SOP tentang pemanfaatan infrastruktur *LAN* dan jaringan komunikasi data di perusahaan.
4. Mengembangkan dan memelihara *website internet* dan *intranet* perusahaan.
5. Menganalisis, merencanakan/disain sistem informasi manajemen berbasis komputer yang selaras dengan tujuan, kebutuhan dan proses bisnis perusahaan
6. Membuat kajian perencanaan dan *desain*/arsitektur *DBMS.*
7. Mendefenisikan struktur *database*, struktur penyimpanan, *desain database*, hak *akses user*, integritas data dan efektifitas *akses DBMS.*
8. Memelihara/menjamin koneksitas ke DBMS di lingkungan perusahaan.
9. Merancang dan menjamin sistem keamanan DBMS
10. Mengadakan evaluasi dan uji kelayakan terhadap perangkat lunak *(software)* yang berkaitan dengan SIM berbasis komputer dan *DBMS* yang akan digunakan di perusahaan.
11. Menilai prestasi kerja seluruh karyawan pelaksana yang menjadi tanggung jawabnya.
12. Menyiapkan *draft* laporan pelaksanaan program dan kegiatan Urusan.

g. Kepala Manajemen Risiko

Tugas Pokok :

1. Menyusun pedoman RKAP Manajemen Risiko dan SOP
2. Menyusun anggaran Urusan Manajemen Risiko dan SOP
3. Menyusun dan merevisi pedoman penerapan manajemen risiko
4. Menyusun dan merevisi pedoman evaluasi Manajemen Risiko
5. Memantau dan evaluasi penerapan pedoman manajemen risiko.
6. Memantau kecukupan modal PTPN V terhadap portofolio risiko
7. Mengevaluasi dan melakukan analisa risiko pada pengembangan usaha dan investasi baru yang diusulkan.
8. Memantau posisi/esposure risiko per jenis risiko.
9. Bertindak sebagai fasilitator hasil *risk assessment*.
10. Mengkompilasi hasil *risk assessment*.
11. Mengembangkan budaya sadar risiko di perusahaan.
12. Memfasilitasi penjabaran risk rolerance di level unit kerja *risk owner*.
13. Menyampaikan laporan pengelolaan risiko secara berkala kepada BOD/BOC.
14. Melaksanakan kegiatan monitoring dan evaluasi pelaksanaan SOP Perusahaan sesuai dengan rencana kerja yang sudah dibuat
15. Menyusun laporan pelaksanaan kegiatan monitoring dan evaluasi pelaksanaan SOP Perusahaan yang dilakukan
16. Menilai prestasi kerja Asisten Urusan serta penilaian prestasi kerja seluruh karyawan pelaksana yang dinilai oleh Asisten Urusan.
17. Membuat laporan pelaksanaan program dan kegiatan Urusan Manajemen Risiko

h. Jabatan Urusan Manajemen Risiko

Tugas Pokok :

1. Menyiapkan *draf* pedoman RKAP yang berkaitan dengan Urusan Manajemen Risiko.
2. Menyiapkan *draf program* kegiatan dan anggaran Urusan Manajemen Risiko.

3. Menyusun *draf* pedoman tentang prosedur dan metodologi dalam identifikasi, pengukuran, pengelolaan, dan pengawasan/ pengendalian risiko.
4. Mengumpulkan data dan dokumen untuk identifikasi dan analisis atas risiko-risiko korporasi bersama bagian terkait.
5. Mengumpulan data dan dokumen untuk melakukan pengukuran risiko baik dalam aspek kuantitas maupun kualitas.
6. Mengumpulkan data dan informasi untuk merumuskan sistem pengelolaan risiko bersama bagian teknis terkait.
7. Mengumpulkan data dan melaksanakan *monitoring* dan evaluasi pengelolaan risiko terhadap semua proses bisnis.
8. Menyiapkan *draf* laporan pengelolaan risiko di perusahaan.
9. Menyiapkan *draf* laporan pelaksanaan *program* dan kegiatan Urusan Manajemen Risiko.
10. Menyiapkan *draf* kompilasi seluruh Profil Manajemen Risiko dari SBU/Bagian/Kebun/Pabrik/ Unit yang menjadi laporan Manajemen Risiko ke Direksi
11. Menilai prestasi kerja seluruh karyawan pelaksana yang menjadi tanggung jawabnya.